1. (Original) A computer-implemented method for creating a cryptographically secure network between at least two access systems, the method comprising a switch system performing the steps of:

associating each of a plurality of access systems with a public key from a private-public key pair associated with said access system;

in response to a request from a first access system to transmit data to a second access system:

authenticating the first access system using the public key associated with the first access system;

forming a first cryptographically secure network connection between the authenticated first access system and the switch system;

accepting data from the authenticated first access system via the first cryptographically secure network connection;

authenticating the second access system using the public key associated with the second access system;

forming a second cryptographically secure network connection between the authenticated second access system and the switch system;

and transmitting the data to the authenticated second access system via the second cryptographically secure network connection.

2. (Currently Amended) The method of claim 1 wherein the switch system issues ~~to~~ an access system the access system's private-pubic key pair; and

the switch system authenticates the first access system by receiving a document encyrpted by the first access system using the private key associated with the first access system and successfully decrypting the document using the public key associated with the first access system.

3. (Original) The method of claim 1 wherein the switch system comprises a plurality of nodes securely networked together.

4. (Original) The method of claim 2 wherein the first and second access systems connect to the switch system via different nodes.

5. (Original) The method of claim 1 further comprising the switch system performing the step of:

using a switch system private key, in conjunction with an access system using a corresponding switch system public key, to authenticate the switch system to the access system.

6. (Original) The method of claim 1 wherein the first and second cryptographically secure connections are each implemented by encrypting the data at a layer selected from the group comprising an application layer, a presentation layer, and a session layer of the Open Systems Interconnection reference model.

7. (Original) The method of claim 6 wherein the first and second cryptographically secure network connections are each formed using at least one encryption key from a group comprising a symmetric key, an asymmetric key, and a symmetric session key encrypted with an asymmetric key.

8. (Original) The method of claim 1 wherein the data is encrypted with at least one encryption key for which the switch system does not have access to the encryption key's corresponding decryption key.

9. (Original) The method of claim 1 wherein the data comprises at least one from the group comprising:

a digest of at least a portion of the data;

and a digital signature of the first access system.

10. (Original) The method of claim 1 further comprising the switch system performing the step of storing at least one of the group comprising the data, a digest of at least a portion of the data, and a digital signature.

11. (Original) The method of claim 10 further comprising the switch system performing the step of time-stamping at least one of the group comprising the data, a digest of at least a portion of the data, and a digital signature of the first access system.

12. (Original) The method of claim 1 wherein the switch system interfaces with an application which utilizes the data exchanged between the first and second access systems.

13. (Original) The method of claim 1 wherein at least one of the first and second access systems connects to the switch system via an application proxy.

14. (Original) The method of claim 13 wherein the application proxy processes data initiated from an access system and data intended for the access system based upon predefined policies.

15. (Original) The method of claim 14 wherein the policies for the application proxy are set by the access system.

16. (Original) A switch system for establishing a secure network connection between at least two access systems, the switch system comprising:

at least one node comprising:

a key module for associating each access system with a public key from a private-public key pair associated with said access system;

an authentication module, coupled to the key manager module, for using an access system's public key, in conjunction with the access system using its private key, to authenticate the access system;

and a secure network module, coupled to the authentication module, for establishing a cryptographically secure network connection between the switch system and an authenticated access system, whereby data is received from a first access system via a first secure connection and transmitted to a second access system via a second secure connection.

17. (Original) The system of claim 16 wherein the key module is further adapted to perform the step of:

issuing a private-public key pair to an access system.

18. (Original) The system of claim 16 wherein the authentication module is further adapted to perform the step of:

using a switch system private key, in conjunction with an access system using a corresponding switch system public key, to authenticate the switch system to the access system.

19. (Original) The system of claim 16 wherein the cryptographically secure network connection is implemented by encrypting the data at a layer selected from the group comprising an application layer, a presentation layer, and a session layer of the Open Systems Interconnection reference model.

20. (Original) The system of claim 19 wherein the cryptographically secure network connections are formed using at least one encryption key from the group comprising a symmetric key, an asymmetric key, and a symmetric session key encrypted with an asymmetric key.

21. (Original) The system of claim 16 wherein the data is encrypted with at least one encryption key for which the switch system does not have access to the encryption key's corresponding decryption key.

22. (Original) The system of claim 16 wherein the node further comprises:

a computer-readable medium for storing at least one of the group comprising the data, a digest of at least a portion of the data, and a digital signature of an access system.

23 -38. (Cancelled)

39. (Original) In a computer-readable medium, a computer program product for creating a cryptographically secure network between at least two access systems, the computer-readable medium comprising program code adapted to perform the steps of:

associating each of a plurality of access systems with a public key from a private-public key pair associated with said access system;

in response to a request from a first access system to transmit data to a second access system:

authenticating the first access system using the public key associated with the first access system;

forming a first cryptographically secure network connection between the authenticated first access system and the switch system;

accepting data from the authenticated first access system via the first cryptographically secure network connection;

authenticating the second access system using the public key associated with the second access system;

forming a second cryptographically secure network connection between the authenticated second access system and the switch system;

and transmitting the data to the authenticated second access system via the second cryptographically secure network connection.

40. (Original) The computer readable medium of claim 39 wherein the switch system issues to an access system the access system's private-pubic key pair.

41. (Original) The computer readable medium of claim 39 wherein the switch system comprises a plurality of nodes securely networked together.

42. (Original) The computer readable medium of claim 41 wherein the first and second access systems connect to the switch system via different nodes.

43. (Original) The computer readable medium of claim 39 farther comprising program code adapted to perform the step of:

using a switch system private key, in conjunction with an access system using a corresponding switch system public key, to authenticate the switch system to the access system.

44. (Original) The computer readable medium of claim 39 wherein the first and second cryptographically secure connections are each implemented by encrypting the data at a layer selected from the group comprising an application layer, a presentation layer, and a session layer of the Open Systems Interconnection reference model.

45. (Original) The computer readable medium of claim 44 wherein the first and second cryptographically secure network connections are each formed using at least one encryption key from the group comprising a symmetric key, an asymmetric key, and a symmetric session key encrypted with an asymmetric key.

46. (Original) The computer readable medium of claim 39 wherein the data is encrypted with at least one encryption key for which the switch system does not have access to the encryption key's corresponding decryption key.

47. (Original) The computer readable medium of claim 39 wherein the data further comprises at least one from the group comprising:

a digest of at least a portion of the data;

and a digital signature of the first access system.

48. (Original) The computer readable medium of claim 39 further comprising program code adapted to perform the step of:

storing at least one of the group comprising the data, a digest of at least a portion of the data, and a digital signature.

49. (Original) The computer readable medium of claim 48 further comprising program code adapted to perform the step of:

time-stamping at least one of the group comprising the data, a digest of at least a portion of the data, and a digital signature of the first access system.

50. (Original) The computer readable medium of claim 39 wherein the switch system interfaces with an application which utilizes the data exchanged between the first and second access Systems.

51. (Original) The computer readable medium of claim 39 wherein at least one of the first and second access systems connects to the switch system via an application proxy.

52. (Original) The computer readable medium of claim 51 wherein the application proxy processes data initiated from an access system and data intended for the access system based upon predefined policies.

53. (Original) The computer readable medium of claim 52 wherein the policies for the application proxy are set by the access system.

54. (New) A computer-implemented method for creating a cryptographically secure network between at least two access systems, the method comprising a switch system performing the steps of:

a plurality of access systems, each having a public key from a private-public key pair associated with said access system;

in response to a request from a first access system to transmit data to a second access system:

authenticating the first access system by decrypting a message encrypted by the first access system using one key of a private-public key pair;

forming a first cryptographically secure network connection between the authenticated first access system and the switch system, wherein communications are encrypted by one key of a private-public key pair;

accepting data from the authenticated first access system via the first cryptographically secure network connection, where said data is encrypted by one key of a private-public key pair;

authenticating the second access system by decrypting a message encrypted by the second access system using one key of a private-public key pair;

forming a second cryptographically secure network connection between the authenticated second access system and the switch system;

and transmitting the data to the authenticated second access system via the second cryptographically secure network connection, where said data is encrypted by one key of a private-public key pair.

55. (New) The method of claim 54 wherein the switch system issues an access system the access system's private-pubic key pair.

56. (New) The method of claim 54 wherein the switch system comprises a plurality of nodes securely networked together.

57. (New) The method of claim 56 wherein the first and second access systems connect to the switch system via different nodes.

58. (New) The method of claim 54 further comprising the switch system performing the step of:

using a switch system private key, in conjunction with an access system using a corresponding switch system public key, to authenticate the switch system to the access system.

60. (New) The method of claim 58 wherein the first and second cryptographically secure network connections are each formed using at least one encryption key from a group comprising a symmetric key, an asymmetric key, and a symmetric session key encrypted with an asymmetric key.

61. (New) The method of claim 54 wherein the data is encrypted with at least one encryption key for which the switch system does not have access to the encryption key's corresponding decryption key.

62. (New) The method of claim 54 wherein the switch authenticates the first access system by decrypting a message encrypted by the first access system using the first access system's private-public key pair.

63. (New) The method of claim 54 wherein the switch authenticates the second access system by decrypting a message encrypted by the second access system using the second access system's private-public key pair.

64. (New) The method of claim 54 wherein the switch forms a first cryptographically secure network connection between the authenticated first access system and the switch system, wherein communications are encrypted by the first access system private-public key pair;

65. (New) The method of claim 55 wherein during transmission the data to the authenticated second access system via the second

cryptographically secure network connection is encrypted by said second access system public key pair.

66. (New) The method of claim 54 wherein during transmission the data to the authenticated second access system via the second cryptographically secure network connection is encrypted by said second access system public key pair.

67. (New) The method of claim 65 wherein said plurality of access systems, each has a unique private-public key pair associated with said access system.

68. (New) The method of claim 54 wherein the switch forms a first cryptographically secure network connection between the authenticated first access system and the switch system, wherein communications are encrypted by the switch system private-public key pair.